3.12 CONTROLS OVER SYSTEM IMPLEMENTATION

The final step to implementing the system includes conversion, documentation, training, and

support. To ensure smooth implementation, it is important that users and technical support

people receive adequate training. To facilitate this training, both system and user

documentation need to define the functionality of the system. Activities during Implementation

stage are discussed below.

3.12.1 Procedures Development

Covers who, what, when, where, and how of the implementation process. Installation of new

hardware / software of the new system interfaces with the other systems or is distributed

across multiple software platforms, some final commissioning tests of the production

environment are carried out to prove end to end connectivity. The design of procedures must

match the job/task responsibility of a user within the organizational functional framework. It

should lay down the activities with respect to a task stating the input, process and output

generated thereof.

The auditor is to assess the following in the procedure document design phase:

• The quality of the procedures design must meet the minimum user requirements and the

SRS specifications of the system.

• Change management principles implemented and followed within the organization.

3.58 Information Systems Control and Audit

• The approach followed in testing and implementation of changes into the behavior and

processes of the system.

• Quality of the procedures documentation, system manuals etc, in a consistent and formal

style.

3.12.2 Conversion

It involved the following activities :

• Defines the procedures for correcting and converting data into the new application,

determining what data can be converted through software and what data manually.

• Performing data cleansing before data conversion,

• Identifying the methods to access the accuracy of conversion like record counts and

control totals,

• Designing exception reports showing the data which could not be converted through

software, and

• Establishing responsibility for verifying and signing off and accepting overall conversion

by the system owner.

The conversion strategies are :

• Direct implementation / Abrupt change-over : The old system is suspended on a specific

day and the new system is implemented. It reduces cost of redundant processing but in

case of a failure due to say a system crashes, the old system is also not available for

recovery. In case of small applications, or when migrating from a manual to computer

system, this may be used.

• Parallel implementation : Both the old and new systems are run in parallel to verify if their

output is the same. Then the old system is suspended. Here redundant processing is

costly but reduces risks associated with conversion. But users will face problems in

working with both systems.

• Phased implementation : This strategy consists of implementing the new system in parts.

This makes implementation more manageable. This is also called the phase-in

conversion and provides a steady transition.

• Pilot implementation : The new systems is first implemented in modules of non-critical

units and then moved to larger unit.

Except direct implementation, others strategies are not mutually exclusive. A cautious

combination of the strategies can be adopted, depending on the type of

application/system.

3.12.3 Auditor’s Role

• Has a Data Conversion Plan been drawn up?

Control Objectives 3.59

• Does the Data Conversion Plan :

♦ Describe the data conversion strategy to be followed (e.g. the procedures for

reconciling differing charts of accounts; the sequence of files to be converted; the

conversion timetable; keeping converted data up-to-date)?

♦ Allocate staff to each task (the users should be fully involved) and define specific

roles and responsibilities, including that of signing off successful completion of each

task?

♦ Set out the criteria for identifying and resolving problems on the quality of the

existing data (e.g. undertake file interrogation to identify missing or incompatible

data items in the existing system; define procedures to deal with the correction of

data rejected by the new system)?

♦ Acceptance tests any custom-built software that has been developed to support the

data conversion task?

♦ Define the controls that are to give assurance that data has been transferred

completely and accurately, and correctly posted (e.g. hash and control totals, and

record counts; checking a sample of detailed records back to the old system;

reconciling balances between the two systems)?

♦ Implement an effective separation of roles between those involved in transferring

data and those involved in verifying that it has been correctly transferred

(information security should not be neglected, particularly where financial data is

involved)?

♦ Define procedures to ensure that converted data is kept up-to-date following its

transfer to the new system?

♦ Define backup and recovery procedures for the converted data on the new system

(these procedures will not relate to any processing cycle so they may differ from the

eventual operational procedures)?

♦ Define how the audit trail is to be preserved after cut over; also, how archived data

from the old system will be processed after de-commissioning?

3.12.4 User Final Acceptance testing

The user acceptance test is performed in a secured testing environment where both source

and executable codes are protected. This helps to ensure that unauthorized or last minute

change to the system does not take place without going through the standard system

maintenance process. Here testing is a complete end-to-end test of the operational system

including all manual procedures. It aims to provide the system users with confirmation that:

• the User Requirement Specification (including system performance criteria) has been

met;

• end user and operational documentation is accurate, comprehensive, and usable;

3.60 Information Systems Control and Audit

• supporting clerical procedures work effectively;

• a production-line support functions operate correctly in-line with user expectations;

• Back-up and recovery procedures work effectively.

The acceptance testing is to be undertaken by the end users supported by IT staff and expert

consultants as necessary, and should continue until no errors or shortcomings remain. In

addition to testing system functions, acceptance testing must also test responsiveness with

respect to the performance criteria defined during the Specification Stage. The acceptance

test plan involves :

• Performance testing should address:

♦ average response time : usually defined as the time between the user depressing

the transmit key, and the first character of the reply appearing on the screen, with a

further maximum time specified for the screen to be completed;

♦ maximum response time : the response time that must not be exceeded;

♦ other response times : for example the time to : load an application, accept or move

between fields on the screen, perform a single or multiple update or to run a

complex enquiry

• Volume testing : subjects the system to heavy volumes of data to test whether it can

handle the volume of data specified in a acceptable time-frame;

• Stress testing : subjects the system to heavy loads or stresses (a heavy stress is a peak

volume of data encountered over a short period)

• Security testing : attempts to subvert the system’s security and internal control checks;

• Clerical procedures checking : aims to confirm that all supporting clerical procedures

have been documented and work effectively;

• Back-up and recovery : aims to confirm that software, configuration files, data and

transaction logs can be backed up, either completely or selectively; and also restored

from backup;

On satisfactory completion of user acceptance testing, the Project Board should sign off a

System Acceptance Document to signify that the development process has been completed,

and hand over all the items that will comprise the operational system to the System Owner (in

practice the bulk of it will pass to the computer operations and software maintenance teams)

3.12.5 Auditor’s Role

The auditor is to assure management that both developers and users have thoroughly tested

the system to ensure that it:

• possesses the built-in controls necessary to provide reasonable assurance of proper

operation;

Control Objectives 3.61

• provides the capability to track events through the systems and thus supports audit

review of the system in operation;

• meets the needs of the user and management;

• If the level of testing does not meet standards, the auditor must notify the development

team or management who will then take corrective action;

• What arrangements have been made to ensure that the system has been correctly built

(installed, configured, loaded, etc) before user acceptance testing commences?

• Has an Acceptance Test Plan been drawn up to cover all aspects of testing?

• allocate adequate resources in terms of manpower, time and equipment to

acceptance testing? (A common problem in IT projects is to reduce the time available

for acceptance testing in order to recover from slippage in the overall project

timetable. This can easily result in the implementation of an inadequately tested

system and defective system);

• allocate individual roles and responsibilities for :

♦ managing the test environment? (i.e. environment design; configuration

management; operation and maintenance)

♦ undertaking individual tests and test cycles?

♦ recording test result?

♦ analysing test results and priorit

3.62 Information Systems Control and Audit

• Does user the Acceptance Testing Plan cover all aspects of the User Requirements

Specification?

• Is an adequate audit trail of changes maintained? (is it possible to back-track on a

change to see how it occurred and whether it was correctly authorized?)

• Are regression tests carried out to ensure that previously accepted areas of the new

system continue to work after significant changes have been implemented?

• Has the acceptance-testing programme been signed off by the Project Board on

successful completion? If not, is appropriate remedial action being taken?

3.12.6 User training

Training both the end-users and the IS operations personnel is critical for the efficient and

effective implementation of a system being seamless integrated within the organization

business process. Training would involve manager’s training on overview and application

systems, operational user training on how to use the software, enter the data, and generate

the output and systems training on the technical aspects. Support along with training, ongoing

user support with trained personnel for problem tracking is another important component

needed to ensure a successful implementation.

3.13 SYSTEM MAINTENANCE

System maintenance is an important phase during the implementation of system; day-to-day

operations bring out the strength and weaknesses which may need periodic modification to

meet its objective. Maintenance can be undertaken under the following three categories:

Corrective maintenance : Emergency program fixes and routine debugging-logical errors.

Adaptive maintenance : Accommodations of change-in the user environment.

Perfective maintenance : User enhancements, improved documentation, and recoding for

improving processing efficiency.

The maintenance phase involves making changes to hardware, software, and

documentation to support its operational effectiveness. It includes making changes to

improve a system’s performance, correct problems, enhance security, or address user

requirements. To ensure modifications do not disrupt operations or degrade a system’s

performance or security, organizations should establish appropriate change management

standards and procedures. Maintaining accurate, up-to-date hardware and software

inventories is a critical part of all change management processes. Management should

carefully document all modifications to ensure accurate system inventories. (If material

software patches are identified but not implemented, management should document the

reason why the patch was not installed.)

Control Objectives 3.63

3.13.1 Auditor’s Role

The effectiveness and efficiency of the system maintenance process is evaluated with the

following metrics:

• The ratio of actual maintenance cost per application/operation versus the average of all

applications/process.

• Average time to deliver change requests.

• The number of change requests for the system application that were related to bugs,

critical errors, and new functional specifications.

• The number of production problems per application and per respective maintenance

changes

• The instances of divergence from standard procedures such as undocumented

applications, unapproved design, and testing reductions.

• The quantity of modules returned to development due to errors discovered in acceptance

testing.

• Time elapsed to analyze and fix problems.

The span of maintenance of the information systems is to ensure effective and timely reporting

of the maintenance needs and being carried out in a controlled manner. The Fig. 3.16

highlights the maintenance control activities widely dispersed throughout the organization

when the system involves end-user participation in the use of the information system. An

auditor needs to satisfy the implementation of maintenance activities and substantial resource

consumption.

3.64 Information Systems Control and Audit

Fig. 3.16 : Maintenance Controls

3.13.2 Performance Measurement

Performance measurement is dependent on the business strategy and objectives of the

organization. The factors for measurement metric would involve:

• the value delivered by the IT system;

• the ratio to the cost of IT to the per unit business function;

• the responsive time of the system for a new or change in operations; and

Control Objectives 3.65

• the ongoing costs of the system to maintain its effectiveness.

For a system to be evaluated properly, it must be assessed using system performance

measurements. Common measurements include throughput (Output per unit of time),

Utilization (Percentage of time the system is being productively used, and response time (how

long it takes the system to respond)

3.14 POST IMPLEMENTATION REVIEW

After a development project is completed a post implementation review should be performed

to determine if the anticipated benefits were achieved. Reviews help to control project

development activities and to encourage accurate and objective initial cost and benefit

estimates. The full scope of a post implementation review (“PIR”) will depend largely on the

scale and complexity of the project. The post implementation review should be performed

jointly by the project development team and the appropriate end users or alternatively, an

independent group not associated with the development process, either internal or external,

should carry out the audit, to meet the following objectives:

• Business objectives : delivered within budget and deadline; is producing predicted

savings and benefits, etc.;

• User expectations : user friendly, carries the workload, produces the required outputs,

good response time, reliable, good ergonomics, etc.;

• Technical requirements : capable of expansion, easy to operate and maintain, interfaces

with other systems, low running cost, etc.

The PIR is undertaken after any changes and tuning that are necessary to achieve a stable

system have been completed, and any significant problems have had a chance to surface.

Sufficient time should also be allowed for the system’s users to become familiar with it. These

criteria should be met between six and twelve months after implementation. If the PIR is

delayed beyond twelve months there will be an increasing risk that changing requirements -

leading to further releases of the system - will obscure the outcome from the original

development; also, that the need for a PIR will be overtaken by other priorities.

If there are obvious and significant problems with a new system a PIR may need to be

undertaken sooner than would otherwise have been the case in order to identify the nature of

the problem(s), their case(s), and to recommend a suitable course of action.

3.14.1 The PIR team

In order to achieve an impartial outcome, the team should be substantially independent of the

original system development team. It may therefore be advisable to employ an external IS

consultant to manage the review. It may also be necessary to employ other external support

to assist in evaluating the delivery of technical (e.g. project management, system design) and

specialized functions (e.g. in financial and management accountancy), and to make

appropriate recommendations where necessary. Internal Audit might help assess the

effectiveness of internal controls.

3.66 Information Systems Control and Audit

In order to facilitate control, the PIR should have terms of reference, authorized by the

approving authority, defining the:-

• scope and objectives of the review;

• criteria to be employed in measuring the achievement of objectives;

• management and organisation of the review team;

• Review budget and reporting deadline.

3.14.2 Activities to be undertaken

During a PIR, the team should, according to their terms of reference, review:-

• the main functionality of the operational system against the User Requirements

Specification;

• system performance and operation;

• the development techniques and methodologies employed;

• estimated time-scales and budgets, and identify reasons for variations;

• changes to requirements, and confirm that they were considered, authorised and

implemented in accordance with change and configuration management standards;

• set out findings, conclusions and recommendations in a report for the authorising

authority to consider.

• In addition to reviewing the functionality delivered by the new system, the review team will

also need to look back to the Business Case on which the system was originally based to

confirm that all the anticipated benefits, both tangible and intangible, have been delivered.

This will involve investigating the reasons behind benefits that were not achieved, perhaps

involving recommendations for remedial action, and using survey techniques to establish

the extent to which intangible benefits (such as improved staff morale) have been realised.

It is also possible that the PIR will identify benefits that were not anticipated in the Business

Case. These should be included in the PIR Report as additional justification for the

investment, and to identify benefits that might be realized in other IS development projects.

Following their deliberations on the PIR Report, the authorizing authority may either:

• endorse continuation of the system;

• approve plans to modify the system;

• terminate the system and made arrangements for a new course of action.

3.14.3 Auditor’s Role

The following issues should be considered when judging the effectiveness either of a PIR, or

to form the basis for the auditor to undertake one.

• Interview business users in each functional area covered by the system, and assess their

satisfaction with, and overall use of, the system.

Control Objectives 3.67

• Interview security, operations and maintenance staff and, within the context of their

particular responsibilities, assess their reactions to the system.

• Based on the User Requirements Specification, determine whether the system’s

requirements have been met. Identify the reason(s) why any requirements are not to be

provided, are yet to be delivered, or which do not work properly.

• Confirm that the previous system has been de-commissioned or establish the reason(s)

why it remains in use.

• Review system problem reports and change proposals to establish the number and

nature (routine, significant, major) of problems, and changes being made to remedy

them. The volume of system change activity can provide an indicator of the quality of

systems development.

• Confirm that adequate internal controls have been built into the system, that these are

adequately documented, and that they are being operated correctly. Review the number

and nature of internal control rejections to determine whether there are any underlying

system design weaknesses.

• Confirm that an adequate Service Level Agreement has been drawn up and

implemented. Identify and report on any area where service delivery either falls below

the level specified, or is inadequate in terms of what was specified.

• Confirm that the system is being backed up in accordance with user requirements, and

that it has been successfully restored from backup media.

• Review the Business Case and determine whether:-

• anticipate benefits have/are been achieved;

• any unplanned benefits have been identified;

• costs are in line with those estimated;

• benefits and costs are falling with the anticipated time-frame.

• Review trends in transaction throughput and growth in storage use to identify the

anticipated growth of the system is in line with that forecast.

Control Category Threats/Risks Controls

System

development and

acquisition controls

System development

projects consume

excessive resources.

Long-range strategic master plan,

data processing schedules,

assignment of each project to a

manage and team, project

development plan, project milestones,

performance evaluations, system

performance measurements

(throughput, utilization, response

time), and post-implementation

reviews.

3.68 Information Systems Control and Audit

Change

management

controls

Systems development

projects consume

excessive resources,

unauthorized systems

changes.

Change management control policies

and procedures, periodic review of all

systems for needed changes,

standardized format for changes, log

and review change requests, assess

impact of changes on system

reliability, categories and rank all,

changes, procedures to handle urgent

matters, communicate changes to

management and users, management

approval of changes, assign specific

responsibilities while maintaining

adequate segregation of duties,

control go through all appropriate

steps, these all changes, develop plan

for backing out of mission-critical

system changes, implement a quality

assurance functions and update

documentation and procedures.

Table 3.5 : Summary of Key Maintainability Controls

3.15 CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY

3.15.1 Information Classification

Information classification is the conscious decision to assign a level of sensitivity to

information as it is being created, amended, enhanced, stored, or transmitted. The

classification of the information should then determine the extent to which it needs to be

controlled / secured and is also indicative of its value in terms of Business Assets.

The classification of information and documents is essential if one has to differentiate between

that which is of little (if any) value, and that which is highly sensitive and confidential. When

data is stored, whether received, created or amended, it should always be classified into an

appropriate sensitivity level. For many organizations, a simple 5 scale grade will suffice as

follows:

Information

Classification

Description

Top Secret

Highly sensitive internal information relating to e.g. pending mergers or

acquisitions; investment strategies; plans or designs; that could seriously

damage the organization if such information were lost or made public.

Information classified as Top Secret information has very restricted

distribution and must be protected at all times. Security at this level is the

highest possible.

Control Objectives 3.69

Highly

Confidential

Information that, if made public or even shared around the organization,

could seriously impede the organization’s operations and is considered

critical to its ongoing operations. Information would include accounting

information, business plans, sensitive customer information of bank's,

solicitors and accountants etc., patient's medical records and similar highly

sensitive data. Such information should not be copied or removed from the

organization’s operational control without specific authority. Security at this

level should be very high.

Proprietary

Information of a proprietary nature; procedures, operational work routines,

project plans, designs and specifications that define the way in which the

organization operates. Such information is normally for proprietary use to

authorized personnel only. Security at this level is high.

Internal Use

only

Information not approved for general circulation outside the organization

where its loss would inconvenience the organization or management but

where disclosure is unlikely to result in financial loss or serious damage to

credibility. Examples would include, internal memos, minutes of meetings,

internal project reports. Security at this level is controlled but normal.

Public

Documents

Information in the public domain; annual reports, press statements etc.;

which has been approved for public use. Security at this level is minimal.

Table 3.6 : Classification of Information

3.15.2 Data Integrity

Once the information is classified, the organization has to decide about various data integrity

controls to be implemented. The primary objective of data integrity control techniques is to

prevent, detect, and correct errors in transactions as they flow through the various stages of a

specific date processing program. In other words, they ensure the integrity of a specific

application’s inputs, stored data, programs, data transmissions, and outputs. .Data integrity

controls protect data from accidental or malicious alteration or destruction and provide

assurance to the user that the information meets expectations about its quality and integrity.

Assessing data integrity involves evaluating the following critical procedures :

• Virus detection and elimination software is installed and activated.

• Data integrity and validation controls are used to provide assurance that the information

has not been altered and the system functions as intended

Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data. Ā

e primary objective in ensuring integrity is to protect the data against erroneous input from

authorized users. Ā e auditor should be concerned with the testing of user-developed systems;

changes or the release of data, unknown to the user, could occur because of fl awed design. Ā

e user may assume that the visible output is the only system activity. Ā e possibility that

erroneous data could infest the system is strong. A person other than the designer or user

should test any application that has access to the organization’s data in more than a read-only

3.70 Information Systems Control and Audit

format. Again, this is a critical area if the service desk is outsourcing to an application service

provider. Release of customer information to such an entity must be controlled through

contractual requirements with stiff remedies or penalties if data is compromised.

There are six categories of integrity controls summarized in Table 7.

Control Category Threats/Risks Controls

Source data control Invalid, incomplete, or

inaccurate source data input

Forms design; sequentially

prenumbered forms, turnaround

documents; cancellation and

storage of documents, review for

appropriate authorization;

segregation of duties, visual

scanning; check-digit

verification; and key verification.

Input validation routines Invalid or inaccurate data in

computer-processed

transaction files

As transaction files are

processed, edit programs

check key data fields using

these edit checks, sequence,

field, sign, validity, limit, range,

reasonableness, redundant data,

and capacity checks. Enter

exceptions in an error log;

investigate, correct, and

resubmit chem. On a timely

basis; re-edit them, and prepare

a summary error report.

On-line data entry

controls

Invalid or inaccurate

transaction input entered

through on-line terminals

Field, limit, range,

reasonableness, sign, validity,

and redundant data checks; user

Ids and passwords; compatibility

tests; automatic system date

entry; prompting operators

during data entry, pre-formatting,

completeness test; closed-loop

verification; a transaction log

maintained by the system; clear

error messages, and data

retention sufficient to satisfy

legal requirements.

Data processing and

storage controls

Inaccurate or incomplete data

in computer-processed

master files

Policies and procedures

(governing the activities of data

processing and storage

personnel; data security and

Control Objectives 3.71

confidentiality, audit trails, and

confidentiality agreements);

monitoring and expediting data

entry by data control personnel;

reconciliation of system updates

with control accounts or reports;

reconciliation of database totals

with externally maintained totals;

exception reporting, data

currency checks, default values,

data marching; data security

(data library and librarian,

backup copies of data files

stored at a secure off-site

location, protection against

conditions that could harm

stored data); use of file labels

and write protection

mechanisms, database

protection mechanisms (date

wise administrators, date

dictionaries, and concurrent

update controls); and data

conversion controls.

Output controls Inaccurate or incomplete

computer output

Procedures to ensure that

system outputs conform to the

organization’s integrity

objectives, policies, and

standards, visual review of

computer output, reconciliation

of batch totals; proper

distribution of output; confidential

outputs being delivered are

protected from unauthorized

access, modification, and

misrouting; sensitive or

confidential out-put stored in a

secure area; users review

computer output for

completeness and accuracy,

shred confidential output no

longer needed; error and

exception reports.

3.72 Information Systems Control and Audit

Data transmission

controls

Unauthorized access to data

being transmitted or to the

system itself; system failures;

errors in data transmission

Monitor network to detect week

points, backup components,

design network to handle peak

processing, multiple

communication paths between

network components, preventive

maintenance, data encryption,

routing verification (header

labels, mutual authentication

schemes, callback systems),

party checking; and message

acknowledgement procedures

(echo checks, trailer labels,

numbered batches)

Table 3.7 : Summary of data Integrity Controls

3.15.3 Data Integrity Policies

• Virus-Signature Updating : Virus signatures must be updated immediately when they are

made available from the vendor.

• Software Testing : All software must be tested in a suitable test environment before

installation on production systems.

• Division of Environments : The division of environments into Development, Test, and

Production is required for critical systems.

• Version Zero Software : Version zero software (1.0,2.0, and so on) must be avoided

whenever possible to avoid undiscovered bugs.

• Offsite Backup Storage : Backups older than one month must be sent offsite for

permanent storage.

• Quarter-End and Year-End Backups : Quarter-end and year-end backups must be done

separately from the normal schedule, for accounting purposes

• Disaster Recovery : A comprehensive disaster-recovery plan must be used to ensure

continuity of the corporate business in the event of an outage.

3.15.4 Data Security

Data security encompasses the protection of data against accidental or intentional disclosure

to unauthorized persons as well as the prevention of unauthorized modification and deletion of

the data. Many levels of data security are necessary in an information systems environment;

they include database protection, data integrity, and security of the hardware and software

controls, physical security over the user, and organizational policies. An IS auditor is

responsible to evaluate the following when reviewing the adequacy of data security controls:

Control Objectives 3.73

• Who is responsible for the accuracy of the data?

• Who is permitted to update data?

• Who is permitted to read and use the data?

• Who is responsible for determining who can read and update the data?

• Who controls the security of the data?

• If the IS system is outsourced, what security controls and protection mechanism does the

vendor have in place to secure and protect data?

• Contractually, what penalties or remedies are in place to protect the tangible and

intangible values of the information?

• The disclosure of sensitive information is a serious concern to the organization and is

mandatory on the auditor’s list of priorities.

3.16 SECURITY CONCEPTS AND TECHNIQUES

3.16.1 Cryptosystems

A cryptosystem refers to a suite of algorithms needed to implement a particular form of

encryption and decryption. Typically, a cryptosystem consists of three algorithms : one for key

generation, one for encryption, and one for decryption. The term cipher (sometimes cypher) is

often used to refer to a pair of algorithms, one for encryption and one for decryption.

Therefore, the term "cryptosystem" is most often used when the key generation algorithm is

important. For this reason, the term "cryptosystem" is commonly used to refer to public key

techniques; however both "cipher" and "cryptosystem" are used for symmetric key techniques.

3.16.2 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a cipher (a method for encrypting information)

selected as an official Federal Information Processing Standard (FIPS) for the United States in

1976, and which has subsequently enjoyed widespread use internationally. It is a

mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded

information. Encrypting data converts it to an unintelligible form called cipher. Decrypting

cipher converts the data back to its original form called plaintext. The algorithm described in

this standard specifies both enciphering and deciphering operations which are based on a

binary number called a key. A key consists of 64 binary digits ("0"s or "1"s) of which 56 bits

are randomly generated and used directly by the algorithm. The other 8 bits, which are not

used by the algorithm, are used for error detection. The 8 error detecting bits are set to make

the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit

byte.

Authorized users of encrypted computer data must have the key that was used to encipher the

data in order to decrypt it. The encryption algorithm specified in this standard is commonly

known among those using the standard. The unique key chosen for use in a particular

application makes the results of encrypting data using the algorithm unique. Selection of a

3.74 Information Systems Control and Audit

different key causes the cipher that is produced for any given set of inputs to be different. The

cryptographic security of the data depends on the security provided for the key used to

encipher and decipher the data. Data can be recovered from cipher only by using exactly the

same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm

but do not have the correct key cannot derive the original data algorithmically. However,

anyone who does have the key and the algorithm can easily decipher the cipher and obtain

the original data. A standard algorithm based on a secure key thus provides a basis for

exchanging encrypted computer data by issuing the key used to encipher it to those

authorized to have the data.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit

key size being too small; DES keys have been broken in less than 24 hours. There are also

some analytical results which demonstrate theoretical weaknesses in the cipher. In recent

years, the cipher has been superseded by the Advanced Encryption Standard (AES) In some

documentation, a distinction is made between DES as a standard, and the algorithm, which is

referred to as the DEA (the Data Encryption Algorithm)

3.16.3 Public Key Infrastructure (PKI)

Public key infrastructure, if properly implemented and maintained, can provide a strong means

of authentication. By combining a variety of hardware components, system software, policies,

practices, and standards, PKI can provide for authentication, data integrity, defenses against

customer repudiation, and confidentiality. The system is based on public key cryptography in

which each user has a key pair—a unique electronic value called a public key and a

mathematically related private key. The public key is made available to those who need to

verify the user’s identity.

The private key is stored on the user’s computer or a separate device such as a smart card.

When the key pair is created with strong encryption algorithms and input variables, the

probability of deriving the private key from the public key is extremely remote. The private key

must be stored in encrypted text and protected with a password or PIN to avoid compromise or

disclosure. The private key is used to create an electronic identifier called a digital signature

that uniquely identifies the holder of the private key and can only be authenticated with the

corresponding public key.

Fig. 3.17 : Public key Infrastructure

Control Objectives 3.75

The certificate authority (CA), which may be the financial institution or its service provider,

plays a key role by attesting with a digital certificate that a particular public key and the

corresponding private key belongs to a specific user or system. It is important when issuing a

digital certificate that the registration process for initially verifying the identity of users is

adequately controlled. The CA attests to the individual user’s identity by signing the digital

certificate with its own private key, known as the root key. Each time the user establishes a

communication link with the financial institution’s systems, a digital signature is transmitted

with a digital certificate. These electronic credentials enable the institution to determine that

the digital certificate is valid, identify the individual as a user, and confirm that transactions

entered into the institution’s computer system were performed by that user.

The user’s private key exists electronically and is susceptible to being copied over a network

as easily as any other electronic file. If it is lost or compromised, the user can no longer be

assured that messages will remain private or that fraudulent or erroneous transactions would

not be performed. User AUPs and training should emphasize the importance of safeguarding

a private key and promptly reporting its compromise.

PKI minimizes many of the vulnerabilities associated with passwords because it does not rely

on shared secrets to authenticate customers, its electronic credentials are difficult to

compromise, and user credentials cannot be stolen from a central server. The primary

drawback of a PKI authentication system is that it is more complicated and costly to implement

than user names and passwords. Whether the financial institution acts as its own CA or relies

on a third party, the institution should ensure its certificate issuance and revocation policies

and other controls discussed below are followed.

When utilizing PKI policies and controls, financial institutions need to consider the following:

• Defining within the certificate issuance policy the methods of initial verification that are

appropriate for different types of certificate applicants and the controls for issuing digital

certificates and key pairs;

• Selecting an appropriate certificate validity period to minimize transactional and

reputation risk exposure—expiration provides an opportunity to evaluate the continuing

adequacy of key lengths and encryption algorithms, which can be changed as needed

before issuing a new certificate;

• Ensuring that the digital certificate is valid by such means as checking a certificate

revocation list before accepting transactions accompanied by a certificate;

• Defining the circumstances for authorizing a certificate’s revocation, such as the

compromise of a user’s private key or the closing of user accounts;

• Updating the database of revoked certificates frequently, ideally in real-time mode;

• Employing stringent measures to protect the root key including limited physical access to

CA facilities, tamper-resistant security modules, dual control over private keys and the

process of signing certificates, as well as the storage of original and back-up keys on

computers that do not connect with outside networks;

3.76 Information Systems Control and Audit

• Requiring regular independent audits to ensure controls are in place, public and private

key lengths remain appropriate, cryptographic modules conform to industry standards,

and procedures are followed to safeguard the CA system;

• Recording in a secure audit log all significant events performed by the CA system,

including the use of the root key, where each entry is time/date stamped and signed;

• Regularly reviewing exception reports and system activity by the CA’s employees to

detect malfunctions and unauthorized activities; and

• Ensuring the institution’s certificates and authentication systems comply with widely

accepted PKI standards to retain the flexibility to participate in ventures that require the

acceptance of the financial institution’s certificates by other CAs.